GAU 2185 #2

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D.C. 20231, on the date indicated below.

Janice E. Favreau
Name of Person Mailing Paper or Fee

Signature — Date of Signature: 4/3/01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of	
Shigeaki Yamane et al.	
for PORTABLE RECORDING MEDIUM AND METHOD OF USING PORTABLE RECORDING MEDIUM	Group Art Unit: 2185
	Our Docket No: 6609-01
Serial No: 09/781,839	
Filed On: February 12, 2001	

Hartford, Connecticut, April 3, 2001

Assistant Commissioner
for Patents
Washington, D. C. 20231

SUBMISSION OF CERTIFIED COPY
UNDER 35 USC §119 AND 37 CFR §1.55(a)

S I R:

Submitted herewith is a certified copy of Japanese Patent Application No. 2000-036399 which was filed on February 15, 2000, in accordance with 35 USC §119 and 37 CFR §1.55(a) to form a part of the above-identified application as filed.

Respectfully submitted,

By _____
John C. Linderman
Registration No. 24,420
Attorney for Applicant

McCormick, Paulding & Huber LLP
CityPlace II
185 Asylum Street
Hartford, Connecticut 06103-4102

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　２月１５日

出願番号
Application Number: 特願２０００－０３６３９９

出願人
Applicant (s): ベーステクノロジー株式会社

２００１年　２月　２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３００３８２１

【書類名】　特許願
【整理番号】　P-3648
【提出日】　平成12年 2月15日
【あて先】　特許庁長官殿
【国際特許分類】　A61B　5/177
【発明者】
　【住所又は居所】　東京都新宿区西新宿７－２２－４５　ベーステクノロジー株式会社内
　【氏名】　山根　茂昭
【発明者】
　【住所又は居所】　東京都新宿区西新宿７－２２－４５　ベーステクノロジー株式会社内
　【氏名】　今城　忠浩
【発明者】
　【住所又は居所】　東京都新宿区西新宿７－２２－４５　ベーステクノロジー株式会社内
　【氏名】　吉田　直邦
【特許出願人】
　【識別番号】　397065952
　【氏名又は名称】　ベーステクノロジー株式会社
【代理人】
　【識別番号】　100080001
　【弁理士】
　【氏名又は名称】　筒井　大和
　【電話番号】　03-3366-0787
【選任した代理人】
　【識別番号】　100093023
　【弁理士】
　【氏名又は名称】　小塚　善高

【選任した代理人】

【識別番号】　100102853

【弁理士】

【氏名又は名称】　鷹野　寧

【手数料の表示】

【予納台帳番号】　006909

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　可搬性記録媒体および可搬性記録媒体の使用方法

【特許請求の範囲】

【請求項１】　アプリケーションソフトウェアと、前記アプリケーションソフトウェアの正当な利用者の個人識別情報と、任意の利用者による前記アプリケーションソフトウェアの使用に先立って前記個人識別情報を用いた個人認証を行う認証ソフトウェアとが格納されていることを特徴とする可搬性記録媒体。

【請求項２】　請求項１記載の可搬性記録媒体において、前記アプリケーションソフトウェアおよび前記認証ソフトウェアは、前記可搬性記録媒体の読み出し専用領域に格納され、前記個人識別情報は、前記可搬性記録媒体の書き換え可能領域に暗号化されて格納されていることを特徴とする可搬性記録媒体。

【請求項３】　請求項１または２記載の可搬性記録媒体において、前記認証ソフトウェアは、前記可搬性記録媒体に格納されている前記個人識別情報と、任意の前記利用者が入力した個人識別情報を照合することで前記個人認証を行う第１の認証機能と、前記可搬性記録媒体に格納されている前記個人識別情報と任意の前記利用者が入力した個人識別情報との照合を、情報ネットワークを介して外部の認証サーバーに依頼し、前記認証サーバーから照合結果を受け取ることで前記個人認証を行う第２の認証機能の少なくとも一方を含むことを特徴とする可搬性記録媒体。

【請求項４】　請求項１，２または３記載の可搬性記録媒体において、前記個人識別情報は、前記利用者の指紋情報であることを特徴とする可搬性記録媒体。

【請求項５】　アプリケーションソフトウェアが格納された可搬性記録媒体に、前記アプリケーションソフトウェアの正当な利用者の個人識別情報を格納しておき、任意の利用者による前記可搬性記録媒体の前記アプリケーションソフトウェアの使用に先立って前記個人識別情報を用いた個人認証を行うことで、正当な前記利用者に、前記可搬性記録媒体に格納されている前記アプリケーションソフトウェアを使用させることを特徴とする可搬性記録媒体の使用方法。

【請求項６】　請求項５記載の可搬性記録媒体の使用方法において、前記ア

プリケーションソフトウェアとともに前記可搬性記録媒体に格納されている認証ソフトウェアを用いて前記個人認証を行うことを特徴とする可搬性記録媒体の使用方法。

【請求項７】　請求項６記載の可搬性記録媒体の使用方法において、前記アプリケーションソフトウェアとともに前記可搬性記録媒体に格納されている前記認証ソフトウェアは、前記可搬性記録媒体に格納されている前記個人識別情報と、任意の前記利用者が入力した個人識別情報を照合することで前記個人認証を行う第１の認証機能と、前記可搬性記録媒体に格納されている前記個人識別情報と任意の前記利用者が入力した個人識別情報との照合を、情報ネットワークを介して外部の認証サーバーに依頼し、前記認証サーバーから照合結果を受け取ることで前記個人認証を行う第２の認証機能の少なくとも一方を含むことを特徴とする可搬性記録媒体の使用方法。

【請求項８】　請求項７記載の可搬性記録媒体の使用方法において、前記認証サーバーは、複数の前記個人識別情報の各々と、個々の前記アプリケーションソフトウェアのライセンスキーとが対応付けて格納されたライセンスデータベースを持ち、前記個人識別情報に対応した前記ライセンスキーを前記照合結果として前記認証ソフトウェアの前記第２の認証機能に応答することで、前記可搬性記録媒体に格納された前記アプリケーションソフトウェアの利用機能の制限を行うことを特徴とする可搬性記録媒体の使用方法。

【請求項９】　請求項５，６，７または８記載の可搬性記録媒体の使用方法において、前記個人識別情報は、前記利用者の指紋情報であることを特徴とする可搬性記録媒体の使用方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、可搬性記録媒体およびその使用技術に関し、特に、高度かつ多様なセキュリテイ管理を必要とするアプリケーションソフトウェアが格納された可搬性記録媒体等に適用して有効な技術に関する。

【０００２】

【従来の技術】

たとえば、いわゆるインターネット等の情報ネットワークの発達および高性能のパーソナルコンピュータの広範な普及に伴い、パーソナルコンピュータを取引端末とする、電子商取引や、証券、金融サービスが普及してきている。

【０００３】

このようなパーソナルコンピュータを取引端末とする上述の各種サービスは、特定のパーソナルコンピュータに備えられた固定ディスク装置（ＨＤＤ）等の外部記憶装置に当該サービス専用の端末ソフトウェア（アプリケーションソフトウェア）を実装して行われることが多い。

【０００４】

【発明が解決しようとする課題】

ところで、特定のパーソナルコンピュータに端末ソフトウェアを実装して利用する場合には、当該サービスの利用場所が特定のパーソナルコンピュータの設置場所に制約され、利用者にとって利便性に欠ける、という技術的課題がある。

【０００５】

さらに、実際のサービス利用に先立って、パーソナルコンピュータへのソフトウェアのインストール作業が必須となり、パーソナルコンピュータの知識に乏しい一般の利用者にとってはサービス利用の敷居が高くなり、サービス普及の障害となるとともに利便性にも欠ける。

【０００６】

一方、最近では、ＣＤ－ＲＷ（Compact Disc-Rewritable）、ＭＯ（Magneto Optical disc）、ＤＶＤ（Digital Versatile Disc）等に代表される書き換え可能な可搬性の大容量記憶媒体が利用可能になってきている。特に、ＣＤ－ＲＷは、媒体価格およびドライブ価格ともに安価で、かつ前世代のＣＤ－ＲＯＭも利用可能なことから急速に普及している。

【０００７】

そこで、このＣＤ－ＲＷ等の大容量可搬媒体に各種サービスに専用の端末ソフトウェアを纏めて実装しておき、任意のパーソナルコンピュータに装填されたＣＤ－ＲＷ上から直接に任意の端末ソフトウェアを立ち上げることで、パーソナル

コンピュータの設置場所に制約されないポータビリティの高いサービスを実現することが考えられる。

【０００８】

ところが、大容量可搬媒体は、ポータビリティが高いが故に、紛失、盗難等のリスクが常に付きまとい、通常のパスワードによる管理では、本人確認等のセキュリティ管理が不十分となる。このため、電子商取引や、証券、金融サービス等のように高いセキュリティを要求されるサービスには適用が躊躇される。

【０００９】

このセキュリティ対策として、たとえば、利用者に複雑なパスワードを設定させることが考えられるが、パスワードの暗唱や秘匿等、利用者のパスワード管理負担が大きくなる、という別の技術的課題を生じる。

【００１０】

本発明の目的は、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用を可能にする可搬性記録媒体およびその使用技術を提供することにある。

【００１１】

本発明の他の目的は、利用者にパスワード管理等の負担をかけることなく、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用を可能にする可搬性記録媒体およびその使用技術を提供することにある。

【００１２】

本発明の他の目的は、高いポータビリティおよびセキュリティにて、多様なライセンスレベルでのアプリケーションソフトウェアの利用を可能にする可搬性記録媒体およびその使用技術を提供することにある。

【００１３】

【課題を解決するための手段】

本発明は、アプリケーションソフトウェアが格納される可搬性記録媒体に、指紋等の個人識別情報を予め登録しておき、この個人識別情報を用いた個人認証により、真正のユーザーのみにアプリケーションソフトウェアの利用を可能ならし

るものである。

【００１４】

すなわち、本発明の可搬性記録媒体は、アプリケーションソフトウェアと、アプリケーションソフトウェアの正当な利用者の個人識別情報と、任意の利用者によるアプリケーションソフトウェアの使用に先立って個人識別情報を用いた個人認証を行う認証ソフトウェアとが格納されるようにしたものである。

【００１５】

また、本発明の可搬性記録媒体の使用方法は、アプリケーションソフトウェアが格納された可搬性記録媒体に、アプリケーションソフトウェアの正当な利用者の個人識別情報を格納しておき、任意の利用者による可搬性記録媒体のアプリケーションソフトウェアの使用に先立って個人識別情報を用いた個人認証を行うことで、正当な利用者に、可搬性記録媒体に格納されているアプリケーションソフトウェアを使用させるものである。

【００１６】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照しながら詳細に説明する。

【００１７】

（実施の形態１）

図１は、本発明の一実施の形態である可搬性記録媒体の構成の一例を示す概念図であり、図２および図３は、本実施の形態の可搬性記録媒体の使用方法の一例を示すフローチャートである。

【００１８】

本実施の形態では、可搬性記録媒体の一例として、ＣＤ－ＲＷを例に採って説明する。

【００１９】

本実施の形態のＣＤ－ＲＷ１０００は、データの記憶領域が、読み出し専用の物理アクセスプロテクトエリア１００１と、書き換え可能なリライタブルエリア１００２にて構成されている。

【００２０】

物理アクセスプロテクトエリア１００１は、後述の各種ソフトウェアの書き込み時に、書き換え不能なデータ書き込み方式を用いてデータ書き込みが実行されており、物理的に、書き換え等による改竄が不可能になっている。

【００２１】

リライタブルエリア１００２は、ソフトウェアによる暗号化にて書き込みデータの保護が行われるプロテクトエリア１００２－１と、ユーザーや後述のアプリケーションプログラムが自由にアクセス可能なフリーエリア１００２－２からなる。

【００２２】

物理アクセスプロテクトエリア１００１には、ユーザー認証プログラム１０、指紋認証エンジン２０、２フェーズ認証プログラム３０、トレーサー４０、アプリケーション管理プログラム５０、複数のアプリケーションソフトウェア５０Ａ、等が格納されている。

【００２３】

ユーザー認証プログラム１０は、後述のように、外部から入力されるユーザーの指紋情報と、予め登録されている指紋情報とに基づいて真正のユーザーを判別する処理を行うソフトウェアであり、ユーザーＩＤ管理機能１０－１、指紋情報管理機能１０－２、認証要求機能１０－３等の機能を備えている。

【００２４】

指紋認証エンジン２０は、ユーザー認証プログラム１０の配下で指紋情報の照合処理を行うソフトウェアであり、入力された指紋情報および登録されている指紋情報から各々の特徴情報を抽出する指紋データ抽出機能２０－１、および特徴情報の照合による一致／不一致の判定を行う指紋照合機能２０－２等の機能を備えている。

【００２５】

２フェーズ認証プログラム３０は、後述のような外部の認証サーバーに指紋照合を依頼する等の認証処理を行うソフトウェアであり、認証サーバー連携機能３０－１等を備えている。

【００２６】

トレーサー４０は、指紋による認証プロセスの監視や記録等の処理を行うものであり、後に不正アクセスの解析等を行うべく、たとえば認証が不成功に終わったときに入力された指紋情報等を記録する指紋データ収集機能４０－１等を備えている。

【００２７】

アプリケーション管理プログラム５０は、後述の２フェーズ認証プログラム３０にて認証サーバー等から得られるライセンスキー等に応じて、各種のアプリケーションソフトウェア５０Ａの各々について、利用可能な機能等の制限を行うためのアプリケーションライセンスキー管理機能５０－１等を備えている。

【００２８】

アプリケーションソフトウェア５０Ａとしては、たとえば、銀行との決済系取引関連のサービスをサポートするバンキング・トランザクションソフトウェア、投資信託、株式、その他の金融商品の運用管理サービスを行うアセット・マネジメントソフトウェア、保険商品サービスを行うライフ・プランニングソフトウェア、投資関連情報、企業情報、等を提供するファイナンシャル・インフォメーションソフトウェア、電子商取引を行うための電子商取引ソフトウェア、等を格納することができる。

【００２９】

リライタブルエリア１００２のプロテクトエリア１００２－１には、ユーザー情報６０、指紋情報７０、ログ情報８０、認証キー情報９０、等が格納される。

【００３０】

ユーザー情報６０は、個々のユーザーにユニークに付与されたユーザーＩＤ６０－１、指紋登録有無フラグ６０－２、等の情報からなる。

【００３１】

指紋情報７０は、後述の登録処理にて得られたユーザーＩＤ７０－１、および指紋データ７０－２、等の情報からなる。

【００３２】

ログ情報８０は、指紋認証処理で照合が不成功に終わったときに得られたユーザーＩＤ８０－１、および指紋データ８０－２、図示しない日時データ等の情報

からなる。

【００３３】

認証キー情報９０は、ユーザーＩＤ９０－１、アプリケーションソフトウェア名９０－２、ライセンスキー９０－３、等の情報からなる。

【００３４】

図６は、本実施の形態の可搬性記録媒体の利用方法にて用いられるパーソナルコンピュータ等の情報処理装置の構成の一例を示す概念図である。

【００３５】

図６のパーソナルコンピュータ２０００において、２００１はマイクロプロセッサ（ＭＰＵ）、２００２はマイクロプロセッサ２００１にて実行されるソフトウェアやデータ等が格納される主記憶、２００３は、固定ディスク装置（ＨＤＤ）等の外部記憶装置、２００４は、外部から装填されるＣＤ－ＲＷ１０００に対するデータの入出力を行うＣＤ－ＲＯＭドライブ、ＣＤ－ＲＷドライブ等の可搬媒体ドライブ、２００５はインターネット等の情報ネットワークに接続されるネットワークインタフェース、２００６はユーザーインタフェース、２００７は指紋等の個人識別情報を取り込むための個人識別情報入力装置、２００８は、これらの各部が接続されるバスである。

【００３６】

個人識別情報入力装置２００７は、たとえば、ユーザーインタフェース２００６を構成するディスプレイ、キーボード、マウス等と一体型の装置でもよいし、これらとは独立な装置形態であってもよい。

【００３７】

主記憶２００２には、たとえば、パーソナルコンピュータ用の汎用オペレーティングシステム２００２ａが常駐し、この汎用オペレーティングシステム２００２ａの上で、ＣＤ－ＲＷ１０００から当該主記憶２００２にロードされる、上述の、アプリケーションソフトウェア５０Ａが稼働する。

【００３８】

以下、本実施の形態の可搬性記録媒体およびその使用方法の作用の一例について説明する。なお、図２において括弧付きで記載されている符号は、当該処理を

実行するプログラムや機能の符号を示している。

【００３９】

まず、図２のフローチャート等を参照して、正当なユーザーの指紋情報のＣＤ－ＲＷ１０００への登録処理について説明する。なお、この登録処理は、たとえば、アプリケーションソフトウェア５０Ａ等をＣＤ－ＲＷ１０００に格納してユーザーに提供する際に、提供者の管理下で正当なユーザーに登録処理を行わせることで、セキュリティが保たれる。

【００４０】

ＣＤ－ＲＷ１０００のユーザーは、当該ＣＤ－ＲＷ１０００を可搬媒体ドライブ２００４に装填することにより、ＯＳ２００２ａの媒体自動起動メカニズムにてＣＤ－ＲＷ１０００を起動し、ユーザー認証プログラム１０、指紋認証エンジン２０等を主記憶２００２にロードして実行する（ステップＳ００１）。

【００４１】

なお、ＣＤ－ＲＷ１０００の起動は、ＯＳ２００２ａの媒体自動起動メカニズムを用いて行わせることに限らず、メニュープログラムを立ち上げて、当該メニュープログラムから行わせるようにしてもよい。

【００４２】

ユーザー認証プログラム１０のユーザーＩＤ管理機能１０－１は、ユーザー情報６０の指紋登録有無フラグ６０－２を参照して、登録済か否かを判定し（ステップＳ００２）、登録済でない場合は、指紋登録を促す認証情報設定画面をユーザーに提示する（ステップＳ００３）。

【００４３】

この画面を見たユーザーは、まず、所定の形式のユーザーＩＤを入力し（ステップＳ００４）、入力された当該ユーザーＩＤは、ユーザーＩＤ管理機能１０－１により、ユーザー情報６０にユーザーＩＤ６０－１として書き込まれる（ステップＳ００５）。

【００４４】

次に、ユーザーは自己の指紋を個人識別情報入力装置２００７にて読み取らせ（ステップＳ００６）、読み取られた指紋情報は、ユーザー認証プログラム１０

にて起動された指紋認証エンジン２０の指紋データ抽出機能２０－１にて特徴情報が指紋データとして抽出され（ステップＳ００７）、抽出された指紋データは、指紋情報管理機能１０－２による暗号化を経て、ユーザーＩＤとともに、ユーザーＩＤ７０－１および指紋データ７０－２として指紋情報７０に格納され（ステップＳ００８）、指紋データ登録処理が完了する。

【００４５】

次に、上述のような登録後における任意の契機でのアプリケーションソフトウェアの利用方法の一例について説明する。

【００４６】

ＣＤ－ＲＷ１０００のユーザーは、当該ＣＤ－ＲＷ１０００を、最寄りのパーソナルコンピュータ２０００の可搬媒体ドライブ２００４に装填することにより、ＯＳ２００２ａの媒体自動起動メカニズムにてＣＤ－ＲＷ１０００を起動し、ユーザー認証プログラム１０、指紋認証エンジン２０等を主記憶２００２にロードして実行する（ステップＳ０１０）。

【００４７】

ユーザー認証プログラム１０のユーザーＩＤ管理機能１０－１は、ユーザー情報６０の指紋登録有無フラグ６０－２を参照して、登録済を確認し（ステップＳ０１１）、正当なユーザーか否かを判別するための指紋認証を行うべく、ユーザーに指紋読み取り処理の実行を促す指紋認証画面をユーザーに提示する（ステップＳ０１２）。

【００４８】

この画面を見たユーザーは、個人識別情報入力装置２００７から自己の指紋を入力し（ステップＳ０１３）、読み取られた指紋から、指紋認証エンジン２０の指紋データ抽出機能２０－１にて特徴情報が指紋データとして抽出され、同時に指紋データ抽出機能２０－１は、指紋情報７０から登録されている指紋データ７０－２を読み出し（ステップＳ０１４）、指紋照合機能２０－２にて、入力された指紋データと登録済の指紋データ７０－２の一致／不一致の照合判定を行い（ステップＳ０１５）、一致すると判定された場合には、ユーザーからの任意のアプリケーションソフトウェア５０Ａの起動要求を受け付け、利用を許可して（ス

テップＳ０１６）、当該アプリケーションソフトウェア５０Ａを、ＣＤ－ＲＷ１０００から読み出して起動し、ユーザーに利用させる（ステップＳ０１７）。

【００４９】

起動されたアプリケーションソフトウェア５０Ａは、稼働に必要なデータおよび稼働中に発生したデータの中でセキュリティ管理必要なデータは、ＣＤ－ＲＷ１０００のプロテクトエリア１００２－１の空き領域を利用して暗号化して書き込み、その他のデータは、フリーエリア１００２－２を利用して記録する。これにより、ＣＤ－ＲＷ１０００のみで稼働する。

【００５０】

なお、上述のように単に、アプリケーションソフトウェア５０Ａを起動して利用させるだけに限らず、たとえば、ユーザー情報６０あるいは指紋情報７０の一部に、任意のアプリケーションソフトウェア５０Ａと、ユーザーＩＤにて特定される特定ユーザー毎のライセンスレベル情報を設定しておき、ステップＳ０１６の起動時に、当該アプリケーションソフトウェア５０Ａにて利用可能な機能に制限を加えることもできる。

【００５１】

ステップＳ０１５で不一致と判定された場合には、入力された指紋データやユーザーＩＤ、日時データ等の経過情報をログ情報８０に記録する（ステップＳ０１８）。このログ情報８０を参照することで、当該ＣＤ－ＲＷ１０００の利用経過や、不正使用の追跡、解析等を的確に行うことが可能になる。

【００５２】

なお、上述の判定処理では、ステップＳ０１３～ステップＳ０１５、ステップＳ０１８を所定の設定回数だけ反復させ、設定回数を超過した場合には、以降の当該ＣＤ－ＲＷ１０００の使用を不能にする処理を加えてもよい。

【００５３】

このように、本実施の形態のＣＤ－ＲＷ１０００およびその使用方法によれば、ＣＤ－ＲＷ１０００に予め登録された指紋等の個人識別情報を用いてユーザー認証を行うので、パスワード管理等の負担をユーザーにかけることなく、高い本人同一性の保証が可能となり、高いセキュリティを実現できる。また、可搬媒体

であるＣＤ－ＲＷ１０００にサービス提供に必要なすべてのアプリケーションソフトウェア５０Ａが格納されているので、ＣＤ－ＲＷ１０００の利点である高いポータビリティと合わせて、ＣＤ－ＲＷ１０００に格納されている多様なアプリケーションソフトウェア５０Ａの簡便な利用を可能にする効果がある。

【００５４】

すなわち、ＣＤ－ＲＷ１０００を携行するユーザーは、最寄りのパーソナルコンピュータ２０００にＣＤ－ＲＷ１０００を装填するだけで、高いセキュリティを必要とする任意のサービスを受けることができる。

【００５５】

この結果、電子商取引や金融関係等、高いセキュリティを必要とするアプリケーションソフトウェア５０Ａの格納および利用に、ＣＤ－ＲＷ１０００を安心して利用でき、高いセキュリティおよびポータビリティによるユーザーおよびサービス提供側の利便性の向上を実現できる。

【００５６】

（実施の形態２）

次に、本発明の可搬性記録媒体の使用方法の他の実施の形態について説明する。

【００５７】

上述の実施の形態１の説明では、ＣＤ－ＲＷ１０００に格納されていたユーザー認証プログラム１００等を用いて、当該ＣＤ－ＲＷ１０００にて閉じた状態で認証処理を行う例を説明したが、指紋の照合や認証処理を外部のサーバー等に依頼することで、より多様なアプリケーションソフトウェア５０Ａの使用における認証管理等を実現することもできる。以下のこのようなＣＤ－ＲＷ１０００の使用方法の一例について説明する。

【００５８】

図４は、本発明の実施の形態２である可搬性記録媒体の使用方法の一例を示すフローチャートであり、図５は、本実施の形態２にて用いられる認証サーバーの構成の一例を示す概念図である。

【００５９】

なお、実施の形態１と同一の構成要素については同一符号で引用することとし、重複する説明は割愛する。

【００６０】

まず、図５にて本実施の形態２における認証サーバー３０００の構成例について説明する。認証サーバー３０００は、制御ソフトウェア３００１として、ユーザー認証プログラム１００、指紋認証エンジン２００、トレーサー３００、アプリケーション利用管理プログラム４００、を備えている。

【００６１】

ユーザー認証プログラム１００は、ユーザーＩＤ管理機能１００－１を備えている。

【００６２】

指紋認証エンジン２００は、指紋照合機能２００－１を備えている。

【００６３】

トレーサー３００は、指紋データ収集機能３００－１を備えている。

【００６４】

アプリケーション利用管理プログラム４００は、アプリケーション利用可否判定機能４００－１、アプリケーション利用ライセンスキー発行管理機能４００－２を備えている。

【００６５】

また、認証サーバー３０００は、データベース３００２として、ユーザー情報５００、ログ情報６００、アプリケーション利用情報７００、等を備えている。

【００６６】

ユーザー情報５００には、認証サーバー３０００の管理者にて登録管理されるユーザーＩＤ５００－１が記録されている。

【００６７】

ログ情報６００には、指紋認証に失敗した認証処理にて得られたユーザーＩＤ６００－１、および指紋データ６００－２、図示しない日時データ等が記録される。

【００６８】

アプリケーション利用情報７００には、認証サーバー３０００の管理者にて登録管理される複数のユーザーＩＤ７００－１と、当該ユーザーＩＤ７００－１に対応して利用許可が設定されたアプリケーションソフトウェア５０Ａのアプリケーションソフトウェア名７００－２、当該アプリケーションソフトウェア５０Ａについて当該ユーザーＩＤ７００－１のユーザーに許可設定された利用の可否や利用レベル等を示すライセンスキー７００－３等が互いに対応付けられて格納されている。

【００６９】

以下、図４のフローチャートにて、本実施の形態２の作用の一例について説明する。なお、図４において括弧付きで記載されている符号は、当該処理を実行するプログラムや機能の符号を示している。

【００７０】

ＣＤ－ＲＷ１０００の起動は、上述の実施の形態１の場合と同様であるが、この実施の形態２の場合には、ユーザー認証プログラム１０および２フェーズ認証プログラム３０が使用される。そして、サービス選択の図示しないメニュープログラムが起動され、実際の各サービスの入口で、ユーザー認証プログラム１０および２フェーズ認証プログラム３０にて、認証サーバー３０００を利用した指紋認証を行う。

【００７１】

すなわち、まず、ＣＤ－ＲＷ１０００の起動時の任意のアプリケーションソフトウェア５０Ａを用いるサービスを選択すると、ユーザー認証プログラム１０によるユーザーからのユーザーＩＤおよび指紋の入力処理が実行され（ステップＳ０２０）、ユーザーから入力された指紋データおよび、図２のフローチャートの処理にて予めＣＤ－ＲＷ１０００に登録されている登録済のユーザーＩＤ７０－１、指紋データ７０－２、当該サービスにて起動されるアプリケーションソフトウェア５０Ａの名前であるアプリケーションソフトウェア名９０－２が、２フェーズ認証プログラム３０の認証サーバー連携機能３０－１にて、認証サーバー３０００に送られる（ステップＳ０２１）。

【００７２】

これを受けた認証サーバー３０００は、ユーザー認証プログラム１００にて、ユーザーＩＤ５００－１とユーザーＩＤ７０－１との照合によるユーザー確認を行った後（ステップＳ０２２）、ユーザーから入力された指紋データと、登録済の指紋データ７０－２との照合を行う（ステップＳ０２３）。

【００７３】

そして、指紋照合結果が一致しない場合には、ユーザー（パーソナルコンピュータ２０００）側から受信した指紋データ等をログ情報６００に、日時データ等とともに記録するとともに（ステップＳ０２４）、当該サービスの利用不可をユーザーに応答する（ステップＳ０２５）。

【００７４】

指紋照合結果が一致した場合には、ユーザー側から受信したアプリケーションソフトウェア名９０－２およびユーザーＩＤ７０－１をキーとしてアプリケーション利用情報７００を参照することで、当該ユーザーによる当該アプリケーションソフトウェア５０Ａの利用の可否を判定し（ステップＳ０２６）、アプリケーション利用情報７００に未登録の場合には、利用不可をユーザー側に応答する（ステップＳ０２７）。

【００７５】

アプリケーション利用情報７００に登録済の場合は、対応するライセンスキー７００－３をアプリケーション利用情報７００から読み出し（ステップＳ０２８）、ユーザー側のアプリケーションライセンスキー管理機能５０－１に送信する（ステップＳ０２９）。

【００７６】

ユーザー側のアプリケーションライセンスキー管理機能５０－１は、当該ライセンスキー７００－３、ユーザーＩＤ７０－１、を、ＣＤ－ＲＷ１０００内の認証キー情報９０に、ユーザーＩＤ９０－１、ライセンスキー９０－３、としてアプリケーションソフトウェア名９０－２と合わせて登録する（ステップＳ０３０）。さらに、当該アプリケーションソフトウェア名９０－２に対応したアプリケーションソフトウェア５０Ａの利用を許可して（ステップＳ０３１）、ＣＤ－ＲＷ１０００から起動する（ステップＳ０３２）。

【００７７】

ユーザーは起動されたアプリケーションソフトウェア５０Ａを用いて、たとえば、インターネット４０００を経由して、各サービスの提供元の図示しないＷｅｂサーバーにアクセスして、所望のサービス提供を受ける（ステップＳ０３３）。

【００７８】

このように本実施の形態２によれば、上述の実施の形態１と同様の効果が得られるとともに、認証サーバー３０００側のアプリケーション利用情報７００のライセンスキー７００－３の設定により、個々のユーザーおよびアプリケーションソフトウェア５０Ａ毎に多様な利用レベルを設定することが可能になる。

【００７９】

また、認証サーバー３０００の側にログ情報６００が残るので、個々のユーザーに所有されているＣＤ－ＲＷ１０００の不正使用の解析やセキュリティ管理をより的確に行うことが可能となる。

【００８０】

以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【００８１】

たとえば、個人識別情報としては、指紋に限らず、声紋、容貌、網膜パターン、筆圧、筆跡等、高いレベルで個人識別が可能な情報を用いることができる。

【００８２】

また、可搬性記録媒体としては、ＣＤ－ＲＷに限らず、ＭＯ、ＤＶＤ、等の可搬性記録媒体、さらには、不揮発性の半導体メモリ等でもよい。

【００８３】

【発明の効果】

本発明の可搬性記録媒体および可搬性記録媒体の使用方法によれば、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用が可能になる、という効果が得られる。

【００８４】

本発明の可搬性記録媒体および可搬性記録媒体の使用方法によれば、利用者にパスワード管理等の負担をかけることなく、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用が可能になる、という効果が得られる。

【００８５】

本発明の可搬性記録媒体および可搬性記録媒体の使用方法によれば、高いポータビリティおよびセキュリティにて、多様なライセンスレベルでのアプリケーションソフトウェアの利用が可能になる、という効果が得られる。

【図面の簡単な説明】

【図１】

本発明の一実施の形態である可搬性記録媒体の構成の一例を示す概念図である。

【図２】

本発明の一実施の形態である可搬性記録媒体の使用方法の一例を示すフローチャートである。

【図３】

本発明の一実施の形態である可搬性記録媒体の使用方法の一例を示すフローチャートである。

【図４】

本発明の他の実施の形態である可搬性記録媒体の使用方法の一例を示すフローチャートである。

【図５】

本発明の他の実施の形態である可搬性記録媒体の使用方法にて用いられる認証サーバーの構成の一例を示す概念図である。

【図６】

本発明の一実施の形態である可搬性記録媒体の利用方法にて用いられるパーソナルコンピュータ等の情報処理装置の構成の一例を示す概念図である。

【符号の説明】

１０　ユーザー認証プログラム
１０－１　ユーザーＩＤ管理機能
１０－２　指紋情報管理機能
１０－３　認証要求機能
２０　指紋認証エンジン
２０－１　指紋データ抽出機能
２０－２　指紋照合機能
３０　２フェーズ認証プログラム
３０－１　認証サーバー連携機能
４０　トレーサー
４０－１　指紋データ収集機能
５０　アプリケーション管理プログラム
５０－１　アプリケーションライセンスキー管理機能
５０Ａ　アプリケーションソフトウェア
６０　ユーザー情報
６０－１　ユーザーＩＤ
６０－２　指紋登録有無フラグ
７０　指紋情報
７０－１　ユーザーＩＤ
７０－２　指紋データ
８０　ログ情報
８０－１　ユーザーＩＤ
８０－２　指紋データ
９０　認証キー情報
９０－１　ユーザーＩＤ
９０－２　アプリケーションソフトウェア名
９０－３　ライセンスキー
１００　ユーザー認証プログラム
１００－１　ユーザーＩＤ管理機能

２００　指紋認証エンジン
２００－１　指紋照合機能
３００　トレーサー
３００－１　指紋データ収集機能
４００　アプリケーション利用管理プログラム
４００－１　アプリケーション利用可否判定機能
４００－２　アプリケーション利用ライセンスキー発行管理機能
５００　ユーザー情報
５００－１　ユーザーＩＤ
６００　ログ情報
６００－１　ユーザーＩＤ
６００－２　指紋データ
７００　アプリケーション利用情報
７００－１　ユーザーＩＤ
７００－２　アプリケーションソフトウェア名
７００－３　ライセンスキー
１０００　ＣＤ－ＲＷ
１００１　物理アクセスプロテクトエリア
１００２　リライタブルエリア
１００２－１　プロテクトエリア
１００２－２　フリーエリア
２０００　パーソナルコンピュータ
２００１　マイクロプロセッサ
２００２　主記憶
２００２ａ　汎用オペレーティングシステム
２００３　外部記憶装置
２００４　可搬媒体ドライブ
２００５　ネットワークインタフェース
２００６　ユーザーインタフェース

２００７　個人識別情報入力装置

２００８　バス

３０００　認証サーバー

３００１　制御ソフトウェア

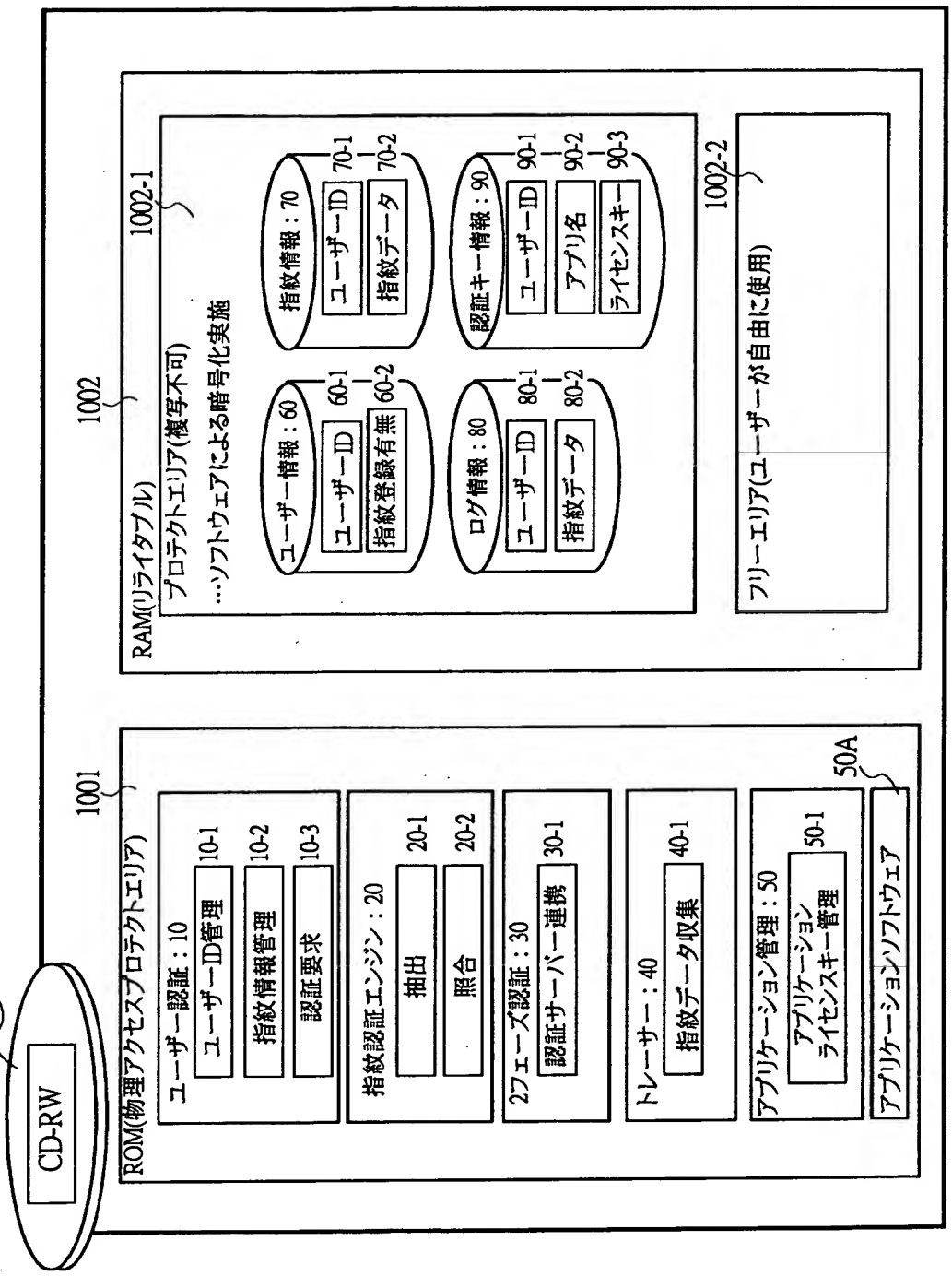
３００２　データベース

４０００　インターネット

【書類名】　図面

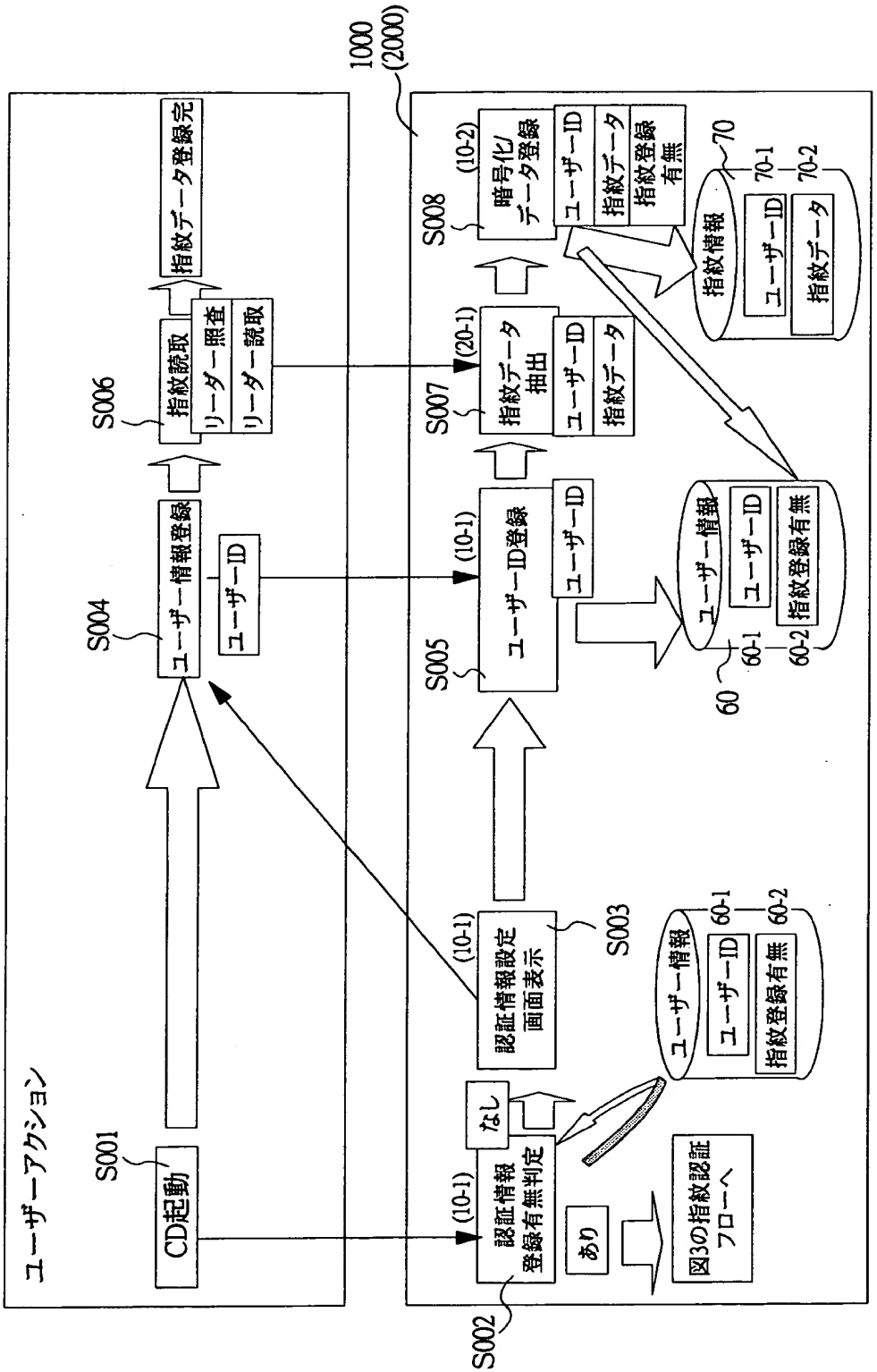
【図１】

図　1


1000
CD-RW
1001
ROM(物理アクセスプロテクトエリア)
ユーザー認証：10
ユーザーID管理
10-1
指紋情報管理
10-2
認証要求
10-3
指紋認証エンジン：20
抽出
20-1
照合
20-2
2フェーズ認証：30
認証サーバー連携
30-1
トレーサー：40
指紋データ収集
40-1
アプリケーション管理：50
アプリケーション
ライセンスキー管理
50-1
50A
アプリケーションソフトウェア
1002
RAM(リライタブル)
1002-1
プロテクトエリア(複写不可)
...ソフトウェアによる暗号化実施
ユーザー情報：60
ユーザーID
60-1
指紋登録有無
60-2
ログ情報：80
ユーザーID
80-1
指紋データ
80-2
指紋情報：70
ユーザーID
70-1
指紋データ
70-2
認証キー情報：90
ユーザーID
90-1
アプリ名
90-2
ライセンスキー
90-3
1002-2
フリーエリア(ユーザーが自由に使用)

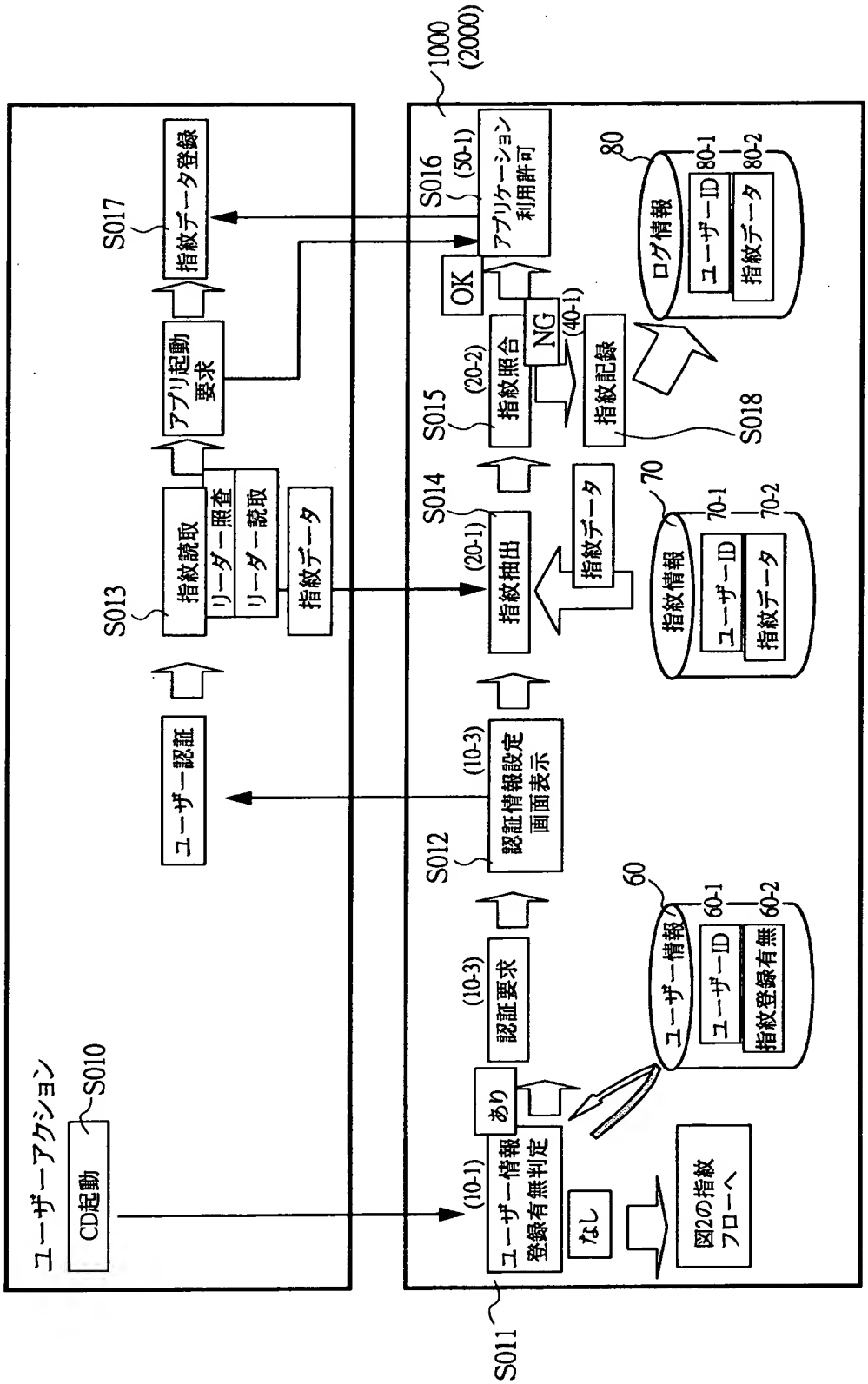
【図２】

図 2


ユーザーアクション
1000
(2000)
S001
CD起動
S002
(10-1)
認証情報
登録有無判定
なし
あり
図3の指紋認証
フローへ
S003
(10-1)
認証情報設定
画面表示
S004
ユーザー情報登録
ユーザーID
S005
(10-1)
ユーザーID登録
ユーザーID
S006
指紋読取
リーダー照査
リーダー読取
指紋データ登録完
S007
(20-1)
指紋データ
抽出
ユーザーID
指紋データ
S008
(10-2)
暗号化/
データ登録
ユーザーID
指紋データ
指紋登録
有無
60
ユーザー情報
ユーザーID
指紋登録有無
60-1
60-2
70
指紋情報
ユーザーID
指紋データ
70-1
70-2

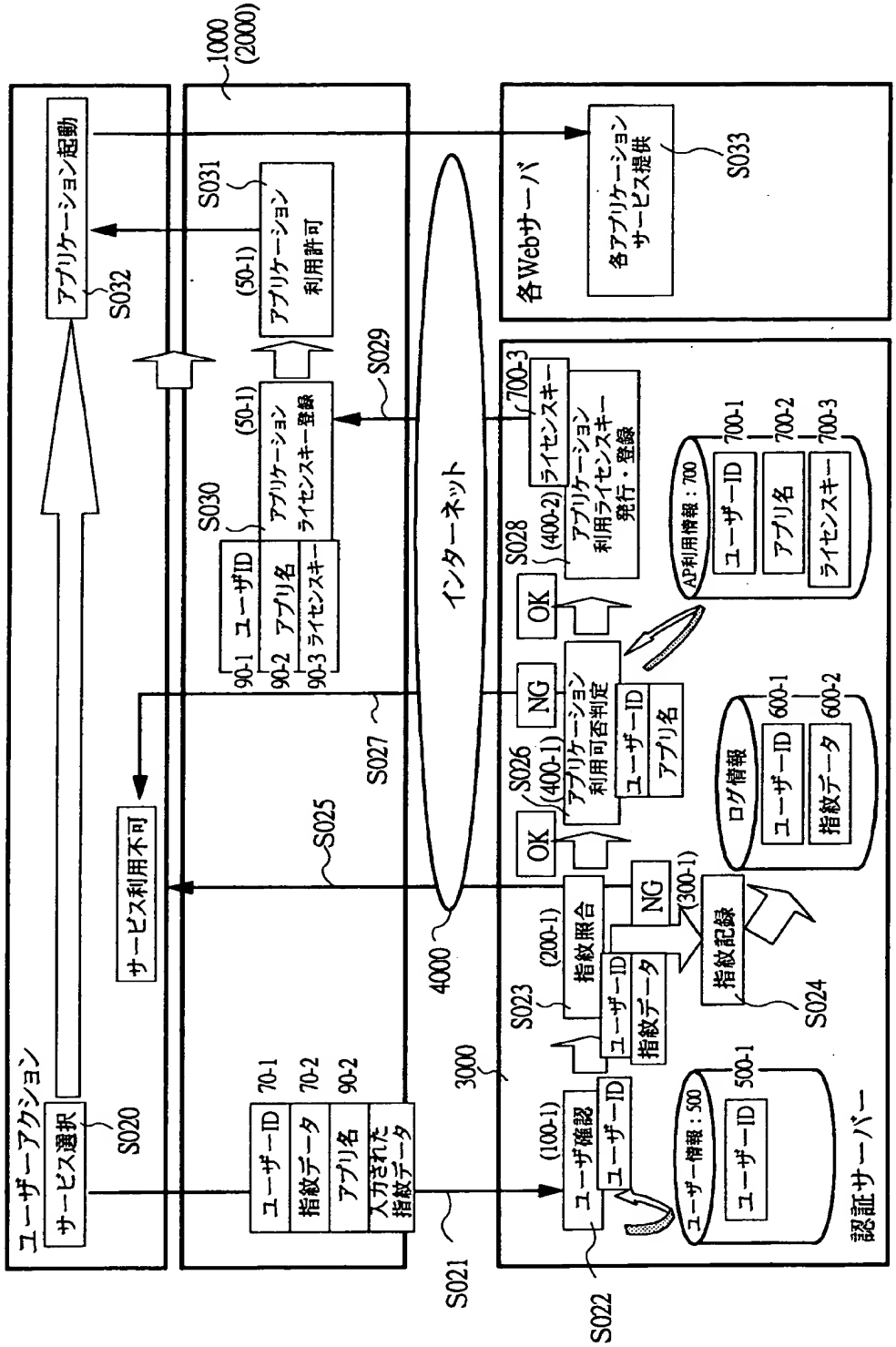
【図３】

図 3


ユーザーアクション
S010
CD起動
S011
(10-1)
ユーザー情報登録有無判定
なし
図2の指紋フローへ
あり
(10-3)
認証要求
S012
(10-3)
認証情報設定画面表示
ユーザー認証
S013
指紋読取
リーダー照査
リーダー読取
指紋データ
S014
(20-1)
指紋抽出
指紋データ
S015
(20-2)
指紋照合
NG
(40-1)
OK
S016
(50-1)
アプリケーション利用許可
S017
指紋データ登録
アプリ起動要求
S018
指紋記録
1000
(2000)
60
ユーザー情報
60-1
ユーザーID
60-2
指紋登録有無
70
指紋情報
70-1
ユーザーID
70-2
指紋データ
80
ログ情報
80-1
ユーザーID
80-2
指紋データ

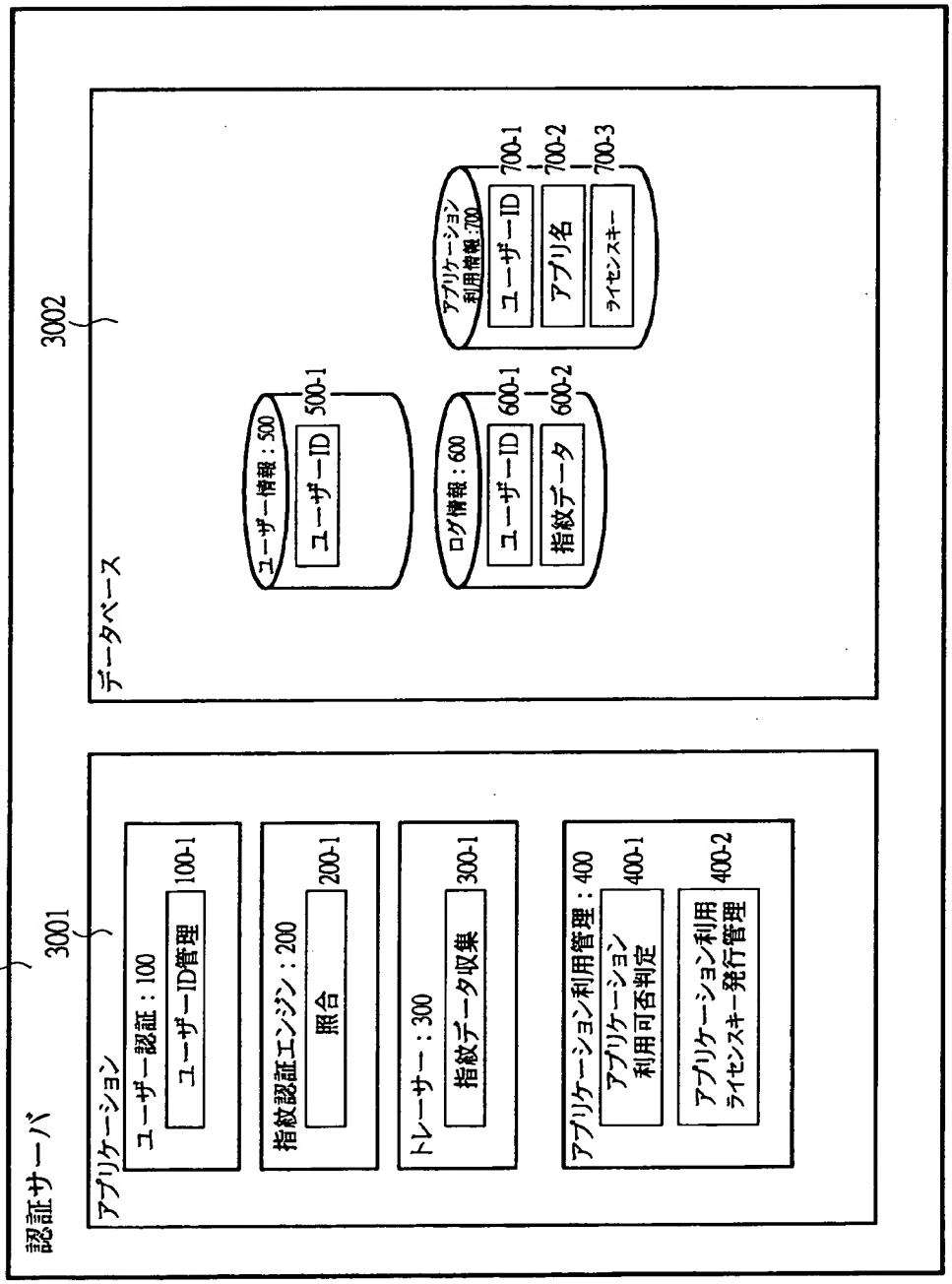
【図４】

図 4


ユーザーアクション
サービス選択
S020
アプリケーション起動
S032
サービス利用不可
S025
1000
(2000)
S031
(50-1)
アプリケーション
利用許可
S029
(50-1)
アプリケーション
ライセンスキー登録
S030
90-1 ユーザID
90-2 アプリ名
90-3 ライセンスキー
ユーザーID
指紋データ
アプリ名
入力された
指紋データ
70-1
70-2
90-2
S021
インターネット
4000
S027
各Webサーバ
各アプリケーション
サービス提供
S033
700-3
ライセンスキー
アプリケーション
利用ライセンスキー
発行・登録
(400-2)
S028
OK
NG
アプリケーション
利用可否判定
(400-1)
S026
OK
ユーザーID
アプリ名
AP利用情報：700
700-1
ユーザーID
700-2
アプリ名
700-3
ライセンスキー
ログ情報
600-1
ユーザーID
600-2
指紋データ
3000
S023
(200-1)
指紋照合
ユーザーID
指紋データ
NG
(300-1)
指紋記録
S024
(100-1)
ユーザ確認
ユーザーID
S022
ユーザー情報：500
500-1
ユーザーID
認証サーバー

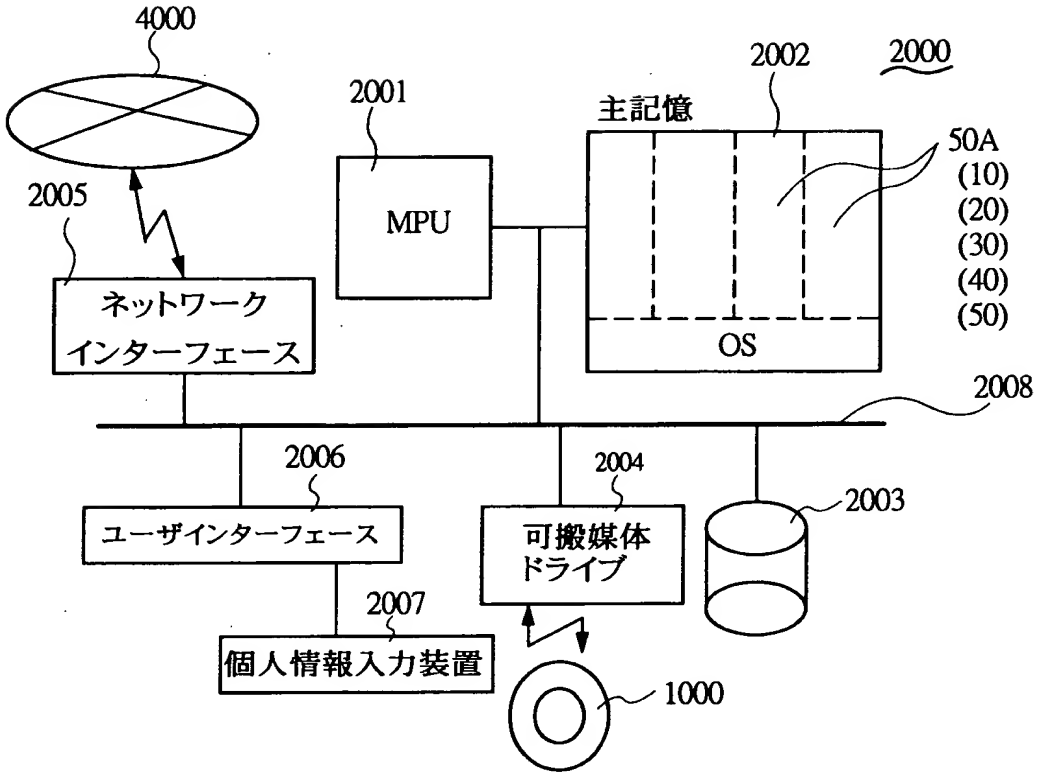
【図５】

図 5


認証サーバ
3000
3001
アプリケーション
ユーザー認証：100
ユーザーID管理
100-1
指紋認証エンジン：200
照合
200-1
トレーサー：300
指紋データ収集
300-1
アプリケーション利用管理：400
アプリケーション
利用可否判定
400-1
アプリケーション利用
ライセンスキー発行管理
400-2
3002
データベース
ユーザー情報：500
ユーザーID
500-1
ログ情報：600
ユーザーID
600-1
指紋データ
600-2
アプリケーション
利用情報：700
ユーザーID
700-1
アプリ名
700-2
ライセンスキー
700-3

【図６】

図 6


4000
2001
2002
2000
主記憶
50A
(10)
(20)
(30)
(40)
(50)
2005
MPU
ネットワーク
インターフェース
OS
2008
2006
2004
2003
ユーザインターフェース
可搬媒体
ドライブ
2007
個人情報入力装置
1000

【書類名】　要約書

【要約】

【課題】　可搬性記録媒体を用いて、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用を可能にする。

【解決手段】　ＣＤ－ＲＷ１０００に読み出し専用の物理アクセスプロテクトエリア１００１と、書き換え可能なリライタブルエリア１００２を設け、物理アクセスプロテクトエリア１００１には、複数のアプリケーションソフトウェア５０Ａと、指紋照合によるユーザー認証を行うためのユーザー認証プログラム１０、指紋認証エンジン２０、等を格納し、リライタブルエリア１００２の複写不可のプロテクトエリア１００２－１には、登録された指紋データ７０－２と、対応するユーザーＩＤ７０－１が格納された指紋情報７０を格納し、指紋照合によるユーザー認証、および認証後のアプリケーションソフトウェア５０Ａの利用が、一つのＣＤ－ＲＷ１０００内で完結するようにした。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔３９７０６５９５２〕

１．変更年月日　　１９９７年１０月２１日
［変更理由］　新規登録
住　所　　東京都新宿区西新宿７－２２－４５
氏　名　　ベーステクノロジー株式会社